

**Management Advisory Report: Annual
Assessment of the Internal Revenue Service's
Information Security - Fiscal Year 2001**

September 2001

Reference Number: 2001-20-191

This report has cleared the Treasury Inspector General for Tax Administration disclosure review process and information determined to be restricted from public release has been redacted from this document.



DEPARTMENT OF THE TREASURY
WASHINGTON, D.C. 20220

INSPECTOR GENERAL
for TAX
ADMINISTRATION

September 28, 2001

MEMORANDUM FOR THE DEPUTY COMMISSIONER FOR MODERNIZATION &
CHIEF INFORMATION OFFICER

A handwritten signature in dark ink, reading "Pamela J. Gardiner".

FROM: Pamela J. Gardiner
Deputy Inspector General for Audit

SUBJECT: Final Management Advisory Report: Annual Assessment of the
Internal Revenue Service's Information Security –
Fiscal Year 2001

This report addresses the following two reporting requirements of the Treasury Inspector General for Tax Administration (TIGTA). First, the Internal Revenue Service (IRS) Restructuring and Reform Act of 1998¹ requires the TIGTA to annually evaluate security in the IRS. This report provides our overall assessment of information security in the IRS. The IRS has made important strides toward improving information security over the past several years. However, IRS systems and taxpayer information are still vulnerable to intruders and unscrupulous employees. We identified weaknesses in controls over external access to Internet gateways, and weaknesses in the IRS' network operating system controls, physical security, and access privileges. While the IRS has policies and procedures to address most security components, they have often been ineffectively implemented.

Second, the Office of Management and Budget (OMB) asked all Inspectors General to provide an assessment of the implementation of the Government Information Security Reform Act² for their respective agencies. In its guidance document, the OMB requested feedback on several security issues. For your information, included as

¹ Internal Revenue Service Restructuring and Reform Act of 1998, § 1103, Pub. L. No. 105-206 (1998), 112 Stat. 685.

² National Defense Authorization, Fiscal Year 2001, § 1061, Pub L. No. 106-398 (2000), 114 Stat. 1654.

Appendix IV is our input to the Department of the Treasury Office of Inspector General, which will be included in its response to the OMB.

Management's Response: Though we did not make any recommendations, we gave the IRS the opportunity to provide feedback to the contents of this report. Management's response to the draft report is included as Appendix V.

Copies of this report are also being sent to the IRS managers who are affected by the report. Please contact me at (202) 622-6510 if you have questions or Scott Wilson, Assistant Inspector General for Audit (Information Systems Programs), at (202) 622-8510.

**Management Advisory Report: Annual Assessment of the
Internal Revenue Service's Information Security - Fiscal Year 2001**

Table of Contents

Background	Page 1
Overall Assessment of Information Security.....	Page 1
Appendix I – Detailed Objective, Scope, and Methodology	Page 4
Appendix II – Major Contributors to This Report.....	Page 6
Appendix III – Report Distribution List.....	Page 7
Appendix IV – Treasury Inspector General for Tax Administration Report on the Government Information Security Reform Act for the Internal Revenue Service Fiscal Year 2001	Page 8
Appendix V – Management's Response to the Draft Report.....	Page 15

Management Advisory Report: Annual Assessment of the Internal Revenue Service's Information Security - Fiscal Year 2001

Background

The Internal Revenue Service (IRS) is a highly visible target for hackers and disgruntled employees, considering the amount and sensitivity of the data the IRS is charged with protecting, and the amount of revenue it collects each year. The IRS maintains sensitive financial information for over 130 million taxpayers, collects over \$2 trillion in revenue each year, and spends over \$9 billion annually to operate the agency.

The IRS Restructuring and Reform Act of 1998¹ requires the Treasury Inspector General for Tax Administration (TIGTA) to annually evaluate security in the IRS. Our assessment for Fiscal Year 2001 is presented below. Also, the Office of Management and Budget (OMB) asked all Inspectors General to provide an assessment of the implementation of the Government Information Security Reform Act² for their respective agencies. In its guidance document, the OMB requested feedback on several security issues. Appendix IV presents our input to the Department of the Treasury Office of Inspector General for inclusion in its response to the OMB.

Most of the information contained in our assessment and the input for the OMB was based on the 20 TIGTA audit reports issued in Fiscal Years 2000 and 2001 on information security. A list of those reports is included in Appendix I. Each of those audits was conducted in accordance with *Government Auditing Standards*.

Overall Assessment of Information Security

The IRS has made strides toward improving security over information systems. The overall security environment of the large processing centers has improved. Mainframe computer operating system controls are generally adequate and significant progress has been made in preparing adequate disaster recovery plans. The IRS has also taken actions to protect its critical information systems. During the last year, the agency has identified the critical assets,

¹ Internal Revenue Service Restructuring and Reform Act of 1998, § 1103, Pub. L. No. 105-206 (1998), 112 Stat. 685.

² National Defense Authorization, Fiscal Year 2001, § 1061, Pub L. No. 106-398 (2000), 114 Stat. 1654.

**Management Advisory Report: Annual Assessment of the
Internal Revenue Service's Information Security - Fiscal Year 2001**

assessed the vulnerability of those assets, and requested funds to improve the physical security of the assets.

Despite the IRS' significant efforts and accomplishments over the past few years, the level of security over information systems in the IRS is not yet adequate based on the vulnerabilities our audits continue to identify. Several of our audits have focused on the adequacy of controls to prevent hackers from intruding into IRS systems or networks, and on controls to detect those who try. Other audits have focused on controls inside the IRS environment.

At the Internet gateways, which control external access into the IRS network, firewalls and routers were not upgraded to protect against commonly known weaknesses, configurations were weak, changes to configurations were not documented, activity logs were not generated and reviewed, and sufficient and capable staffing was not assigned to administer the firewalls. The IRS does not have the capability to detect intrusions at all entry points from the Internet.

Internally, we noted weaknesses with network operating system controls, physical security, and access privileges. Due to the interconnectivity of systems within the IRS, these weaknesses are significant. Unauthorized persons gaining access to a computer in even the smallest post-of-duty can potentially access data in any of the computing centers. The IRS still does not routinely run or review activity logs on network servers to detect potential internal security breaches.

The IRS does have policies and procedures to address most security components. However, our audit findings indicate that these policies and procedures have often been ineffectively implemented due to a lack of clear accountability for security throughout the IRS, insufficient knowledge and skills, insufficient security awareness among managers and employees, and inadequate certification and accreditation processes.

Accountability for implementing and testing security has been given primarily to the Office of Security under the direction of the Deputy Commissioner for Modernization

**Management Advisory Report: Annual Assessment of the
Internal Revenue Service's Information Security - Fiscal Year 2001**

and Chief Information Officer. This is contrary to the OMB's policy of charging functional officials with ultimate responsibility for security over the systems they manage. Functional managers have not routinely reviewed their systems to identify physical, operational and detection control weaknesses as required by the Security Act. In an organization as large and decentralized as the IRS, it is highly unlikely that a relatively small organization such as the Office of Security can effectively carry out these duties.

In several of our audits, we noted that managers and employees, particularly those with key security responsibilities, did not have sufficient knowledge and skills to carry out their security responsibilities. We could not readily determine the training provided to employees because the IRS' training information was unreliable.

The IRS provides its employees with annual briefings designed to heighten awareness of disclosure laws regarding unauthorized accesses to taxpayer information. However, managers and employees were not sufficiently aware of many other security risks and their personal responsibilities for ensuring security. In a recent test, TIGTA representatives emulated a hacker attack by posing as help desk employees. Seventy-one of 100 employees indicated that they were willing to change their passwords to one recommended by the TIGTA representative. Hackers could use these passwords to gain access into the IRS network.

Over the years, the IRS has not routinely considered security when designing new systems. When we completed our first audit of the security certification process in June 2000, we knew of only one operational system that had been rolled out with its security requirements completed. As of May 2001, the IRS had made little progress in clearing its backlog of sensitive systems that need certification. About 85 percent of the 252 systems that process or store sensitive data had either not received a certification at all or needed re-certification. However, the IRS has recently taken steps to ensure that certification is obtained before new systems are implemented, and has enlisted contractor support in an attempt to clear the backlog for systems already in operation.

Detailed Objective, Scope, and Methodology

This report presents the Treasury Inspector General for Tax Administration's (TIGTA) annual assessment of information security in the Internal Revenue Service. This annual assessment is required by the Internal Revenue Service Restructuring and Reform Act of 1998.¹ Most of the information contained in the assessment was based on the following 20 TIGTA audit reports issued from February 2000 to July 2001 on information security.

The Internal Revenue Service Can Improve Information Systems Physical Security (Reference Number 2000-20-039, dated February 2000) (Limited Official Use)

The Internal Revenue Service Needs to Complete Disaster Recovery and Business Resumption Plans (Reference Number 2000-20-031, dated March 2000) (Limited Official Use)

The Internal Revenue Service Can Improve Software-Based Access Controls to Enhance Security for Local Area Networks (Reference Number 2000-20-073, dated April 2000) (Limited Official Use)

The Internal Revenue Service Needs to Develop Security Policies for Local Area Networks (Reference Number 2000-20-074, dated May 2000) (Limited Official Use)

The General Controls Over a Critical Internal Revenue Service Tax Processing Computer System Can Be Strengthened (Reference Number 2000-20-072, dated May 2000) (Limited Official Use)

Certifying the Security of Internal Revenue Service Computer Systems is Still a Material Weakness (Reference Number 2000-20-092, dated June 2000)

The Security and Performance of Electronic Tax Return Processing Should Be Improved to Meet Future Goals (Reference Number 2000-20-095, dated June 2000)

A Comprehensive Program for Preventing and Detecting Computer Viruses is Needed (Reference Number 2000-20-094, dated June 2000) (Limited Official Use)

The Internal Revenue Service Should Improve Actions to Protect Its Critical Infrastructure (Reference Number 2000-20-097, dated June 2000) (Limited Official Use)

Computer Security Controls Should Be Strengthened in the Houston District (Reference Number 2000-20-106, dated July 2000)

¹ Internal Revenue Service Restructuring and Reform Act of 1998, § 1103, Pub. L. No 105-206 (1998), 112 Stat. 685.

**Management Advisory Report: Annual Assessment of the
Internal Revenue Service's Information Security - Fiscal Year 2001**

Security Over Taxpayer Data Used in Conducting Compliance Research Should Be Improved (Reference Number 2000-20-159, dated September 2000)

Computer Security Controls Should Be Strengthened in the Former Brooklyn District (Reference Number 2001-20-020, dated November 2000) (Limited Official Use)

The Control Environment Over the Consolidated Computer Systems for Collection Activities Needs to be Strengthened (Reference Number 2001-20-034, dated December 2000) (Limited Official Use)

Computer Security Controls Should Be Strengthened in the Former Northern California District (Reference Number 2001-20-036, dated January 2001) (Limited Official Use)

Security Over Data From the Department of Health and Human Services Should Be Improved (Reference Number 2001-20-065, dated April 2001) (Limited Official Use)

Disaster Recovery Plans for Mainframe Systems at the Tennessee Computing Center Have Improved, But Mid-Range Systems Still Need Attention (Reference Number 2001-20-072, dated April 2001) (Limited Official Use)

Controls Over the Masterfile System Are Generally Adequate, But Some Improvement Is Needed (Reference Number 2001-20-092, dated June 2001) (Limited Official Use)

Controls Over the Internet Gateway Should Be Improved to Better Deter and Detect External Attacks (Reference Number 2001-20-101, dated June 2001) (Limited Official Use)

Persistent Physical Security Vulnerabilities Should Be Corrected to Better Protect Facilities and Computer Resources (Reference Number 2001-20-108, dated July 2001) (Limited Official Use)

Letter Report: Planning Efforts to Protect Critical Infrastructure Facilities Are Adequate (Reference Number 2001-20-111, dated July 2001)

Major Contributors to This Report

Scott E. Wilson, Assistant Inspector General for Audit (Information Systems Programs)
Stephen Mullins, Director
Kent Sagara, Audit Manager
Bret Hunter, Senior Auditor
William Lessa, Senior Auditor
William Simmons, Auditor

Report Distribution List

Commissioner N:C
Deputy Commissioner N:DC
Chief, Information Technology Services M:I
Director, Office of Security M:S
Chief Counsel CC
Director, Legislative Affairs CL:LA
Director, Office of Program Evaluation and Risk Analysis N:ADC:R:O
National Taxpayer Advocate TA
Office of Management Controls N:CFO:F:M
Audit Liaison:
 Deputy Commissioner for Modernization & Chief Information Officer M

**Treasury Inspector General for Tax Administration
Report on the Government Information Security Reform Act
for the Internal Revenue Service
Fiscal Year 2001**

On October 30, 2000, the President signed into law the Fiscal Year (FY) 2001 Defense Authorization Act, Pub. L. No. 106-398, including Title X, subtitle G, "Government Information Security Reform Act (the Security Act)." The Office of Management and Budget (OMB) provided guidance that directed each agency head and the agency's Inspector General to provide the OMB with an executive summary on how the agency is implementing requirements of the Security Act.

OMB requested the Inspectors General to comment on the agencies' actual performance rather than the measures of performance requested in several of the questions below. In addition, the Inspectors General were only requested to respond to items 2-13. This report contains the Treasury Inspector General for Tax Administration's comments related to the Internal Revenue Service (IRS).

1. *Identify the agency's total security budget as found in the agency's FY01 budget request, FY01 budget enacted, and the FY02 budget request.*

We were not requested to comment on this topic.

2. *Identify the total number of programs included in program reviews or independent evaluations.*

The IRS Office of Security reported that, from October 1999 to May 2001, it performed 41 reviews at IRS facilities, including monthly reviews at remittance processing operations, physical reviews of contractor sites and reviews of lockbox bank sites. These reviews assessed the physical, logical, personnel and network security environments. We did not evaluate the adequacy of the Office of Security's reviews.

The TIGTA conducted reviews at 42 facilities that focused on security controls for 8 mainframe, 26 mid-range, 18 network computers, and one major Internet gateway. We also conducted physical security reviews at each of the 42 facilities. We have issued 20 final reports addressing information security in the last two years. (A list of these reports is included in Appendix I.)

**Management Advisory Report: Annual Assessment of the
Internal Revenue Service's Information Security - Fiscal Year 2001**

3. *Describe the methodology used in the program reviews and the methodology used in independent evaluations.*

We applied the five levels of program effectiveness from the Federal Information Security Assessment Framework, published by the Federal CIO Council and the National Institute of Standards and Technology (NIST). This methodology determines whether (1) policies are documented, (2) procedures are documented, (3) procedures and controls are implemented, (4) procedures and controls are tested and reviewed, and (5) procedures and controls are fully integrated. We also considered policies and guidelines provided by the NIST, the General Accounting Office (GAO), and the Department of the Treasury in evaluating the adequacy of security in the IRS. All of our reviews followed *Government Auditing Standards*, as established by the GAO.

4. *Report any material weakness in policies, procedures, or practices as identified and required to be reported under existing law.*

As of June 2001, the IRS had reported four material weaknesses regarding information security (Sensitive System Certification, District Office Security, Service Center Security and Other IRS Facility Security). Each of these material weaknesses has been reported for several years. The latter three weaknesses were reported in 1997, soon after the Office of Security was formed. At that time, management consolidated several weaknesses by the type of facility. The IRS has developed multi-year plans to correct each of the weaknesses. Currently, the Sensitive System Certification weakness is being monitored on a monthly basis by the IRS' Financial and Management Control Executive Steering Committee.

In June 2000, the TIGTA issued a report entitled, "*Certifying the Security of Internal Revenue Service Computer Systems Is Still a Material Weakness.*" The report stated that 90 percent of the IRS' 258 sensitive systems had not been certified. We attributed this condition primarily to the lack of emphasis the IRS had placed on building security controls into new information systems. It had become a standard practice in the IRS to implement a system without the necessary certification and accreditation of security controls. We were aware of only one information system in use that had been certified and accredited before it had been implemented.

Since the above report was issued, the IRS has considered process improvements for certifying new systems before implementation and for redefining certification requirements. Management has also enlisted contractor support to assist in the certification process. We have not yet evaluated these actions. However, to date, the IRS has made very little progress in clearing its backlog of sensitive systems that need certification. This includes systems that have never been certified and those that need re-certification. As of May 2001, 85 percent of the systems currently defined as

**Management Advisory Report: Annual Assessment of the
Internal Revenue Service's Information Security - Fiscal Year 2001**

sensitive had either not received initial certification or needed re-certification. Because the IRS has a large number of sensitive systems, and with the requirement to re-certify systems every 3 years or when significant modifications are made, it will be difficult to catch up. For example, since January 2000, 132 certifications have expired and only 25 of those systems are in the process of being re-certified. We plan to follow up on this issue in early FY 2002.

5. *Describe the specific measures of performance used by the agency to ensure that agency program officials have: (1) assessed the risk to operations and assets under their control; (2) determined the level of security appropriate to protect such operations and assets; (3) maintained an up-to-date security plan for each system supporting the operations and assets under their control; and (4) tested and evaluated security controls and techniques. Include information on the actual performance for each of the four categories.*

The four categories in this topic are included in the IRS' sensitive system certification process. As mentioned in the previous topic, the certification of sensitive systems is still a problem. The IRS currently has 252 systems that process or store sensitive data. The Office of Security, which is responsible for maintaining security documentation for the certification of all sensitive systems, did not have any documentation for 34 percent of the sensitive systems. Due to time constraints, we did not follow up with system owners to determine whether certification documents existed for these systems.

Although the Office of Security has conducted some tests, functional offices have not conducted any reviews of their systems as required by the OMB. Guidance provided by the OMB on implementing the Security Act stated that system owners, not the Chief Information Officer (CIO), are ultimately responsible for the security of programs under their control and should conduct annual tests of those systems.

6. *Describe the specific measures of performance used by the agency to ensure that the agency CIO: (1) adequately maintains an agency-wide security program, (2) ensures effective implementation of the program and evaluates the performance of major agency components, and (3) ensures the training of agency employees with significant security responsibilities. Include information on the actual performance for each of the three categories.*

The IRS Office of Security was established in January 1997, under the CIO, and is responsible for establishing and enforcing standards and policies for all major IRS security programs including, but not limited to, physical security, data security, and systems security. During FY 2001, the Commissioner gave security a much higher priority and backed it up by providing additional resources to the Office of Security. We have not recently evaluated the effectiveness of this office but plan a review in FY 2002.

**Management Advisory Report: Annual Assessment of the
Internal Revenue Service's Information Security - Fiscal Year 2001**

In several of our audits, there were issues that indicate a lack of technical expertise by employees with key security responsibilities. For example, weak password configurations and employee non-compliance with security rules were partly caused by a lack of network security training provided to System Administrators and to a lack of awareness of security risks by employees.

7. *Describe how the agency ensures that employees are sufficiently trained in their security responsibilities. Identify the total number of agency employees and briefly describe what types of security training was available during the reporting period, the number of agency employees that received each type of training, and the total costs of providing such training.*

The IRS provides annual briefings to its employees on disclosure laws dealing with unauthorized accesses to taxpayer information. However, the IRS does not have an effective control for ensuring that agency employees are adequately trained on the full range of security issues that affect them. The IRS uses a national database for storing training data on employees; however, the data is not kept current. As a result, the IRS cannot determine the number of employees given security training, what types were available, and the costs of providing security training. The database does not distinguish employees with key security responsibilities from other employees. Accountability for maintaining the database has not been established. We will include employee training in our review of the Office of Security in FY 2002.

8. *Describe the agency's documented procedures for reporting security incidents and sharing information regarding common vulnerabilities. Include a description of procedures for external reporting to law enforcement authorities and to the General Service Administration's FedCIRC. Include information on the actual performance and the number of incidents reported.*

The IRS Incident Response Center has guidelines for how it should handle incidents reported to them. However, IRS field offices have no procedures for handling security incidents. The IRS has recently established and staffed functions to specifically react to incidents as they occur and is currently in the process of developing guidelines for resolving incidents.

In 2001, the IRS reported over 2,000 computer-related incidents to the Department of the Treasury. Most of the incidents involved identification of viruses. The Department of the Treasury did not report any of the incidents to FedCIRC, the government's clearinghouse for identifying widespread attacks on multiple agencies.

**Management Advisory Report: Annual Assessment of the
Internal Revenue Service's Information Security - Fiscal Year 2001**

The IRS started installing and standardizing intrusion detection capabilities in January 2001. As of July 2001, several Internet gateways still did not have this capability. We expect the number of identified incidents to increase significantly once intrusion detection is installed agency-wide.

9. *Describe how the agency integrates security into its capital planning and investment control process. Were security requirements and costs reported on every FY 2002 capital asset plan submitted by the agency to the OMB? If not, why not?*

The IRS Office of Security, within the Office of the CIO, is the information systems security function for the IRS. This office represents a significant portion of the IRS' security-related expenditures relating to oversight and operational controls. The IRS security function's budget requirements are separately identified prior to being integrated into the IRS Commissioner's annual budget request. We did not conduct reviews during the year to identify whether other operating functions within the IRS had security-related costs that should be separately listed in the capital asset plans. Based on information provided by the IRS, security costs are not separately identified in the OMB monitoring vehicles including the capital asset plan and the annual budget. We have scheduled audits in this area for FY 2002 to determine if the IRS is complying with budget reporting requirements.

10. *Describe the specific methodology (e.g., the Project Matrix) used by the agency to identify, prioritize and protect critical assets within its enterprise architecture, including links with key external systems. Describe how the methodology has been implemented.*

The IRS has made significant progress in protecting its critical assets as required by Presidential Decision Directive 63 (PDD 63). PDD 63, signed in May 1998, called for a national effort to ensure the security of the nation's critical infrastructure. The critical infrastructure is defined as systems essential to the minimum operations of the economy and government.

In a report issued in June 2000, we stated that the IRS had not identified its critical assets as required by PDD 63 and accordingly had not identified cyber vulnerabilities and plans to eliminate those vulnerabilities. Subsequently, we reported in July 2001 that the IRS had identified its critical assets and had established plans to reduce the physical vulnerabilities in key facilities.

The Office of Security had coordinated with the National Chief Infrastructure Assurance Officer (CIAO), the Department of the Treasury, and other IRS business units to identify those assets deemed critical to protecting the nation's infrastructure. Computer systems and physical assets required to file returns and to collect revenue were

**Management Advisory Report: Annual Assessment of the
Internal Revenue Service's Information Security - Fiscal Year 2001**

considered as the IRS' critical infrastructure. The Office of Audit has not yet followed up to evaluate the IRS' progress in developing plans to reduce the cyber vulnerabilities.

11. Describe the measures of performance used by the head of the agency to ensure that the agency's information security plan is practiced throughout the life cycle of each agency system. Include information on the actual performance.

The IRS relies on the certification and accreditation process to ensure that security is built into its systems throughout the enterprise life cycle. Current procedures for the sensitive system certification process require all security requirements to be met before a system is rolled out for operation. However, as we mentioned earlier, there are material problems with the certification process. As of June 2000, we knew of only one operational system that had been rolled out with its security requirements completed. In addition, 85 percent of the IRS' sensitive systems currently in operation are not certified and functional officials are not conducting annual program reviews required by the Security Act.

12. Describe how the agency has integrated its information and information technology security programs with its CIP responsibilities and other security programs (e.g. physical and operational.)

The IRS has established the Director, Office of Security, under the CIO, as the IRS' CIAO, per requirements of PDD 63. Also, the IRS is currently formalizing a Critical Infrastructure Management Plan that aims to provide a formal framework to guide individuals and organizational components in performing Critical Infrastructure Protection activities. The primary intent of the plan is to complement, or build on existing foundations, rather than replace existing IRS security and information assurance requirements and procedures.

13. Describe the specific methods (e.g., audits or inspections) used by the agency to ensure that contractor provided services (e.g., network or website operations) or services provided by another agency are adequately secure and meet the requirements of the Security Act, OMB policy, NIST guidance, and agency policy.

We have not conducted any work on contractor support within the IRS during the last 2 years.

**Management Advisory Report: Annual Assessment of the
Internal Revenue Service's Information Security - Fiscal Year 2001**

14. *Each Agency head, working with the CIO and program officials, must provide the following information to OMB: a plan of action with milestones that includes completion dates, describes how the agency plans to address any issues/weaknesses, and identifies obstacles to address known weaknesses.*

We were not requested to comment on this topic.

**Management Advisory Report: Annual Assessment of the
Internal Revenue Service's Information Security - Fiscal Year 2001**

Appendix V

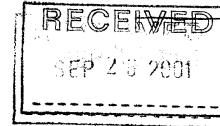
Management's Response to the Draft Report



DEPUTY COMMISSIONER

DEPARTMENT OF THE TREASURY
INTERNAL REVENUE SERVICE
WASHINGTON, D.C. 20224

SEP 26 2001



MEMORANDUM FOR DEPUTY INSPECTOR GENERAL FOR AUDIT

FROM: John C. Reece *Len Baptiste for*
Deputy Commissioner for Modernization &
Chief Information Officer

SUBJECT: Response to Draft Management Advisory Report – Annual
Assessment of the Internal Revenue Service's Information
Security – Fiscal Year 2001 (#200120022)

Thank you for the opportunity to review and comment on the Treasury Inspector General for Tax Administration's draft report concerning its overall assessment of information security in the IRS. We note that your report does not contain any specific recommendations.

However, we agree with your concern that the Office of Security cannot on its own effectively carry out the security responsibilities of functional and business unit managers. As we have briefed your team on our overall approach to security program implementation (the "sandwich" chart), the IRS security program is in the process of defining discrete security accountabilities by security initiative in each of the IRS' operating divisions, shared services units and other operating functions. We are working with these managers to ensure their understanding and compliance with designated security roles and responsibilities. We would be delighted to brief you again, should you be interested.

If you have any questions or concerns, please feel free to contact me at (202) 622-6800 or Mr. Len Baptiste, Director, Office of Security at (202) 622-8910.